IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

THERESA BELLER, on behalf of herself and on behalf of all other similarly situated individuals,

Plaintiff,

v.

THE WACKS LAW GROUP, LLC,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Theresa Beller ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through her undersigned counsel, files this Class Action Complaint against The Wacks Law Group, LLC ("WLG" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of her counsel as to all other matters.

I. INTRODUCTION

1. Plaintiff brings this class action lawsuit against WLG for its failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII").[1] As a result of WLG's insufficient data security,

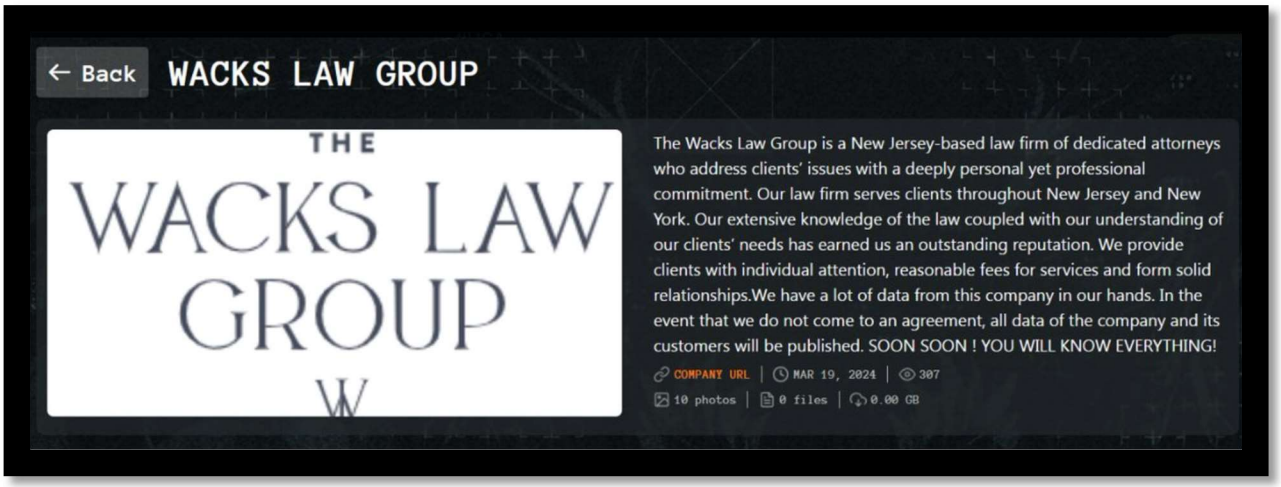
[1] https://mm.nh.gov/files/uploads/doj/remote-docs/wacks-law-group-

cybercriminals easily infiltrated WLG's inadequately protected computer systems, accessing and acquiring the PII of Plaintiff and the Class (the "Data Breach" or "Breach").[2] Now, Plaintiff's and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. According to WLG, on March 9, 2024, it discovered suspicious activity in its network environment.[3]

3. After an investigation, WLG determined that an "unauthorized third party potentially acquired personal information during the Data Breach."[4]

4. Shortly after the Data Breach, ransomware group—Qilin—claimed responsibility for the Data Breach, as pictured below.[5]



20240806.pdf.

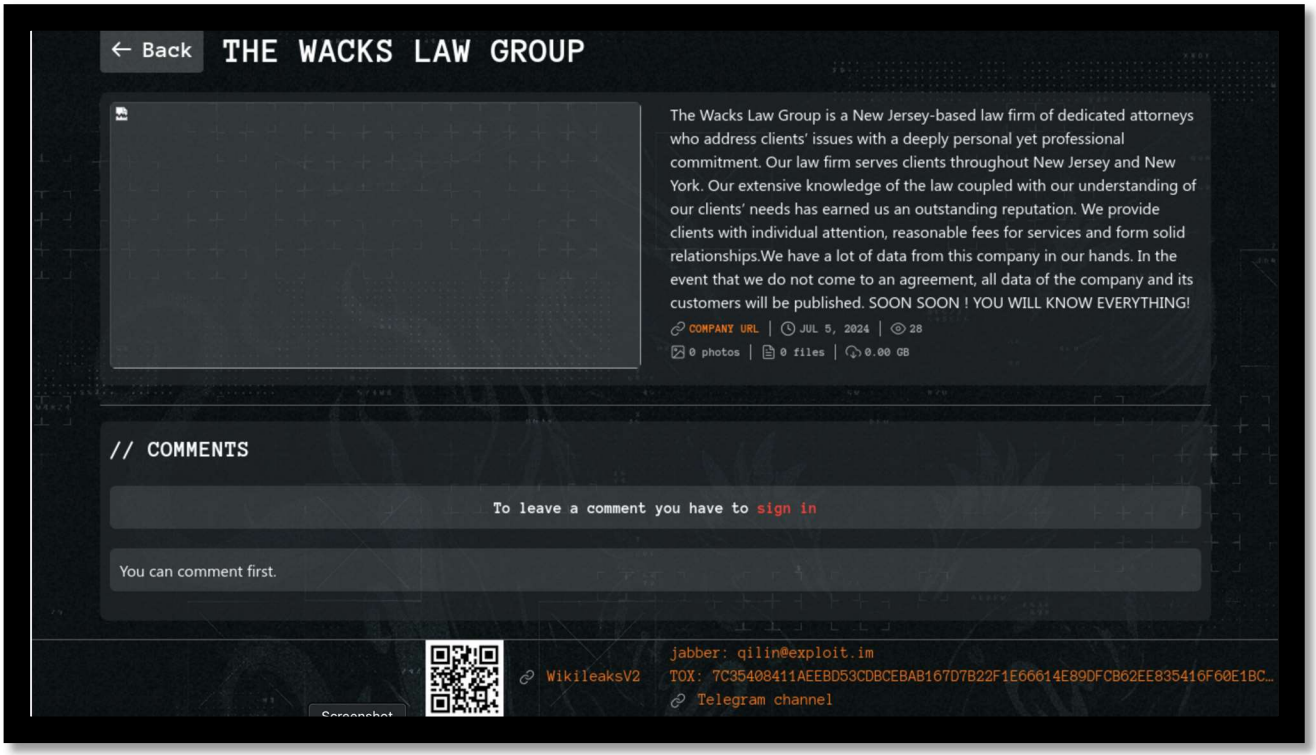
[2] *Id.*

[3] *See* Exhibit 1 (Plaintiff's Notice of Data Breach Letter from WLG).

[4] *Id.*

[5] https://x.com/FalconFeedsio/status/1775825649468379512/photo/1; https://www.breachsense.com/breaches/the-wacks-law-group-data-breach/.

5. The Data Breach was disclosed through Qilin's dark web leak site, where they announced the exfiltration and encryption of sensitive data including PII, confidential documents, and non-disclosure agreements.[6]



6. "Qilin, also known as Agenda, is a ransomware-as-a-service (RaaS) entity that surfaced in 2022. It targets a variety of sectors worldwide, with a particular focus on critical infrastructure. The ransomware utilized by Qilin is noted for its sophistication, written in Rust and Go, which enhances its evasion

[6] https://ransomwareattacks.halcyon.ai/attacks/ransomware-attack-on-the-wacks-law-group-a-legal-firms-vulnerability-to-cyber-threats; https://www.ransomlook.io/screenshots/qilin/The%20Wacks%20Law%20Group.png.

capabilities. Their operations are marked by a double extortion scheme, which not only encrypts the data but also exfiltrates it, posing a dual threat to the victims."[7]

7. The PII subject to unauthorized access and acquisition included highly sensitive PII such as: names, Social Security numbers, and driver's license numbers (collectively, "Private Information").[8] However, the full extent of the stolen information is still unknown.

8. WLG acquired, collected, and stored Plaintiff's and Class Members' Private Information in connection with the legal services it provided. Therefore, at all relevant times, WLG knew or should have known that Plaintiff's and Class Member's sensitive data, including their highly confidential PII would be stored on its networks.

9. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff and the Class. These duties arose from state and federal statutes and regulations as well as common law principles.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII

[7] Id.
[8] *See* Ex. 1.

was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

11. Due to WLG's negligent failure to secure and protect Plaintiff's and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of millions of individuals.

12. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft will have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

13. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit,

diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

14. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

15. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

16. **Plaintiff Theresa Beller** is an individual domiciled in Jacksonville, Florida. Plaintiff received a Notice of Data Breach Letter from WLG dated August 6, 2024, notifying her that her name, Social Security number, and driver's license number were compromised in the Data Breach.[9]

17. Defendant **WLG** is a New Jersey limited liability company with members and managers located within this District. WLG's principal place of business located at 110 South Jefferson Road, Suite 304, Whippany, NJ 07981.

[9] Ex. 1.

III. JURISDICTION AND VENUE

18. Jurisdiction is proper in this Court under 28 U.S.C. § 1332(d). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member, including Plaintiff, is a citizen of a state different from Defendant.

19. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

20. As previously stated, Defendant is a New Jersey limited liability company and has its principal place of business in New Jersey. Defendant also has sufficient minimum contacts in New Jersey and has intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within New Jersey.

21. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1) because a substantial part of the events that gave rise to Plaintiff's claims took place within this District, and Defendant does business and has its principal place of business here.

IV. FACTUAL ALLEGATIONS

A. WLG's Collection of Plaintiff's and the Class's Private Information.

22. WLG is a New Jersey-based law firm that provides estate planning, Medicaid planning, asset preservation planning, businesses services, and other legal services to clients in New Jersey and New York.[10]

23. WLG's focus on estate planning and business representation, combined with its extensive client relationships, made it a prime target for cybercriminals seeking to leverage or monetize stolen data. This shows the need for enhanced cybersecurity measures within the legal sector, particularly for firms handling large volumes of sensitive client information, such as WLG.[11]

24. As part of the legal services WLG provides, it is entrusted with, and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable laws and industry standards.

25. Several legal ethics rules have application to the protection of client information that WLG failed to protect. According to the American Bar Association ("ABA") Rule 1.6: Confidentiality of Information, lawyers must make reasonable efforts to prevent unauthorized access or disclosure of client information.[12]

---

[10] https://wackslaw.net/learn-more-about-planning-your-future-with-the-wacks-law-group.
[11] https://ransomwareattacks.halcyon.ai/attacks/ransomware-attack-on-the-wacks-law-group-a-legal-firms-vulnerability-to-cyber-threats.
[12] https://www.americanbar.org/groups/law_practice/resources/law-technology-

26. Additionally, the ABA has also released several ethics opinions (such as Securing Communication of Protected Client Information and Lawyers' Obligations After an Electronic Data Breach or Cyberattack) that provide guidance for lawyers on how to address cybersecurity.[13]

27. WLG understood the importance of protecting Plaintiff's and the Class's PII and made promises and representations to its clients, including Plaintiff and Class Members, that the Private Information it collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

28. In fact, Defendant provides on its website:

> ***How is Personal Information Protected?***
>
> We take certain appropriate security measures to help protect your personal information from accidental loss and from unauthorized access, use or disclosure.[14]

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes

---

today/2024/ensuring-security-protecting-your-law-firm-and-client-data/#:~:text=According%20to%20the%20American%20Bar,or%20disclosure%20of%20client%20information.

[13] *Id.*

[14] https://wackslaw.net/terms-of-use-and-disclaimer.

only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand adequate data security to safeguard their Private Information.

30. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its clients' Private Information safe and confidential.

31. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Plaintiff's and the Class's Private Information, Defendant could not perform the legal services it provides and obtain revenue.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

34. However, Defendant failed to take this responsibility seriously and failed to protect Plaintiff's and the Class's Private Information from unauthorized access, resulting in a massive and preventable data breach.

B. Defendant's Massive and Preventable Data Breach.

35. According to WLG, on March 9, 2024, WLG became aware of suspicious activity in its network environment.[15]

36. After learning of the Data Breach, WLG claims it initiated an investigation, through which it determined that an "unauthorized third party potentially acquired personal information."[16]

37. Soon after the Data Breach, ransomware group, Qilin, confirmed it stole Plaintiff's and the Class's PII during the Data Breach and posted a sample of it on the dark web.[17]

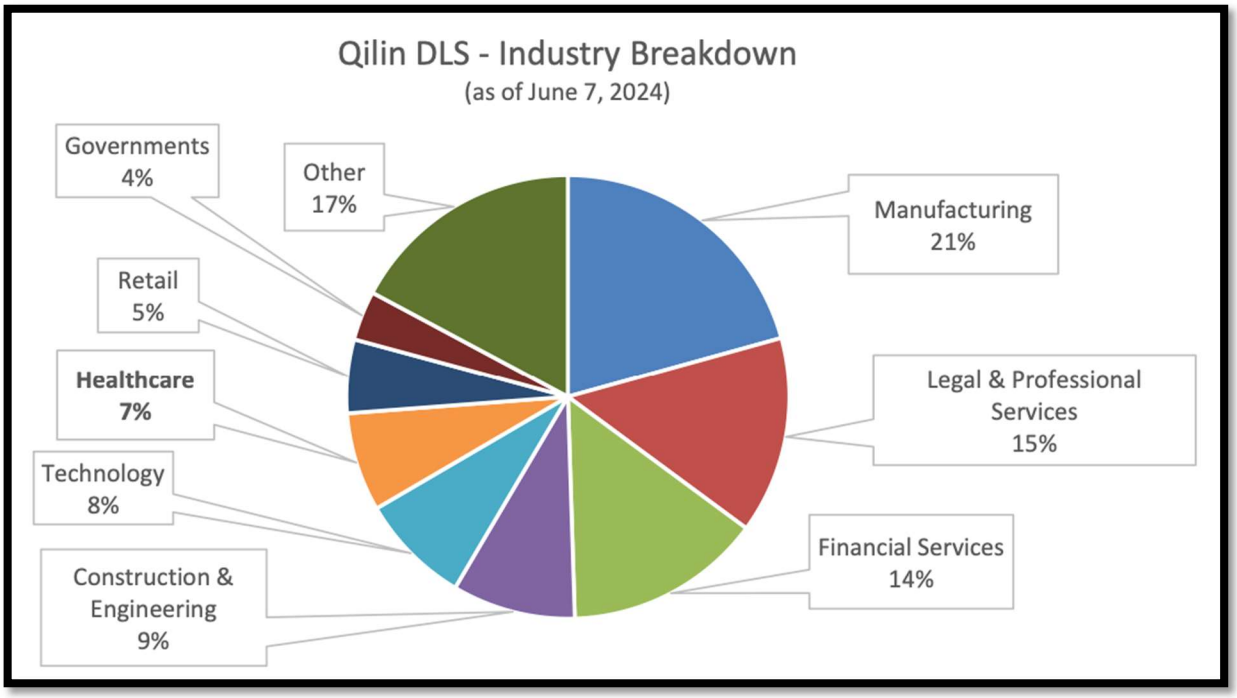
[IMAGE ON FOLLOWING PAGE]

[15]Ex. 1.
[16] *Id.*
[17] https://www.linkedin.com/posts/dexpose_databreach-dataleak-infosec-activity-7181631642246004736-y-FD.

38. "Qilin is a ransomware-as-a-service (RaaS) offering in operation since 2022, and which continues to target healthcare organizations and other industries worldwide. The group likely originates from Russia, and was recently observed recruiting affiliates in late 2023. The ransomware has variants written in Golang and Rust, and is known to gain initial access through spear phishing, as well as leverage

Remote Monitoring and Management (RMM) and other common tools in its attacks. The group is also known to practice double extortion, demanding ransom payments from victims to prevent data from being leaked."[18]

39. Qilin's most targeted industries include manufacturing, legal and professional services—such as WLG—and financial services.[19]



40. On May 22, 2024, WLG identified the persons whose sensitive information was "potentially impacted."[20]

41. The information stolen in the Breach includes highly sensitive PII such as: names, Social Security numbers, and driver's license numbers.[21]

[18] https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf.
[19] *Id.*
[20] Ex. 1.
[21] *Id.*

42. Despite learning of the Data Breach in March 2024, WLG failed to begin notifying victims of the Data Breach until in or around August 2024 via Notice of Data Breach Letters.[22]

43. It is clear WLG expects victims of the Data Breach to experience fraud and identity theft resulting from the Data Breach because WLG states the following in its Notice of Data Breach Letters:[23]

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Information*, to learn more about how to protect against the possibility of information misuse.

44. These are suggestions WLG need not make if there were not an imminent risk of fraud and identity theft.

45. After receiving the Notice Letters, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and that it its necessary for them to take steps to mitigate that substantial risk of impending and future harm. Indeed, Defendant admonishes victims of the Data Breach to "remain vigilant against incidents of identity theft and fraud."[24]

[22] *Id.*
[23] *Id.*
[24] *Id.*

46. Defendant made a token gesture of a mere twelve (12) months of credit monitoring services to Plaintiff and the Class—an offer it need not have provided absent any threat to Plaintiff and the Class.[25] However, this offer is woefully inadequate considering Plaintiff and Class Members will be at a continued risk of fraud and identity theft for the rest of their lives. This gesture does not and will not fully protect Plaintiff and the Class from cybercriminals and is largely ineffective against protecting data after it has been stolen. Cybercriminals are fully aware of the well-publicized preventative measures taken by entities after data breaches such as that which happened here and will, therefore, oftentimes hold onto the stolen data and not use it until after the complimentary service is no longer active, and long after victim concerns and preventative steps have diminished.

47. Upon information and belief, the unauthorized third-party cybercriminals intentionally targeted and gained access to Plaintiff's and the Class's PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII to fraudsters as that is the *modus operandi* of data thieves.

48. The Notice of Data Breach Letter WLG sent to victims of the Data Breach amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts such as

[25] *Id.*

how long the Data Breach occurred, why it took WLG so long to notify affected individuals of the Breach, and who the perpetrator of the Data Breach is and if a ransom demand was paid. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

49. Furthermore, Defendant inexplicably delayed giving notice of the Data Breach to Plaintiff and the Class for months, giving cybercriminals a head-start in misusing and selling Plaintiff's and the Class's Private Information.

50. Defendant did not use reasonable security procedures and practices appropriate to protect the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, which resulted in the access and exfiltration of Plaintiff's and the Class's Private Information.

51. The perpetrator of the Data Breach accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, Social Security numbers, driver's license numbers and other sensitive information.

52. Upon information and belief, the unauthorized third-party cybercriminal(s) gained access to the Private Information and engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiff's and Class Members' Private Information on the dark web.

53. Plaintiff believes that her Private Information and that of Class Members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

54. Plaintiff and Class Members' Private Information was provided to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

55. Accordingly, Defendant had obligations created by the FTC Act, reasonable industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

56. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify threats and defend against them.

57. The stolen Private Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that Social Security numbers were part of the data that was compromised.

C. Plaintiff's Individual Experience.

Plaintiff Beller's Experience

58. Plaintiff Beller received a Notice of Data Breach Letter from Defendant dated August 6, 2024, informing her that her Private Information was compromised in the Data Breach.[26]

59. Defendant was in possession of Plaintiff Beller's Private Information before, during, and after the Data Breach.

60. Because of the Data Breach, Plaintiff Beller's highly confidential Private Information is in the hands of cybercriminals. As such, Plaintiff Beller and the Class are at an imminent risk of identity theft and fraud.

61. As a result of the Data Breach, Plaintiff Beller has already expended hours of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements and other information.

62. Plaintiff Beller places significant value in the security of her PII and does not readily disclose it. Plaintiff Beller has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

[26] *Id.*

63. Plaintiff Beller has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach. Indeed, Defendant acknowledged the increased risk of future harm Plaintiff Beller, and the Class now face by offering complimentary credit monitoring services to Plaintiff Beller and the Class.

64. Knowing that data thieves intentionally targeted and stole her PII, including her Social Security number, and knowing that her PII is in the hands of cybercriminals has caused Plaintiff Beller great anxiety beyond mere worry. Specifically, Plaintiff Beller has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her PII has been stolen.

65. Plaintiff Beller has a continuing interest in ensuring that her PII, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's PII will be wholly unprotected and at-risk of future data breaches.

66. Plaintiff Beller has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals;

(iii) damages to and diminution in value of her Private Information that was entrusted to Defendant for the sole purpose of obtaining services with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Beller should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

D. Defendant had an Obligation to Protect Private Information Under the Law and the Applicable Standard of Care.

67. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

68. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class Members' Private Information.

69. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and email systems to ensure that the Private Information in its possession was adequately secured and protected.

70. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

71. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

72. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

73. Defendant owed a duty to Plaintiff and the Class to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

74. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems, software, and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy

would be a material fact in the decision to entrust Private Information with Defendant.

75. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

76. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

E. Defendant was on Notice of Cyberattack Threats in the Legal Services Industry and of the Inadequacy of its Data Security.

77. WLG was on notice that law firms have been prime targets for cyberattacks.

78. Some of the most notable law firm cyberattacks include: (i) Orrick, Herrington & Sutcliffe; (ii) Grubman Shire Meiselas & Sacks; (iii) Proskauer Rose; (iv) Appleby; and (v) Mossack Fonseca.[27]

79. "Legal practices are a honeypot for cybercriminals. Highly sensitive client information, such as financial records, legal files, or intellectual property, has resale value on the dark web."[28]

80. "Law firms face significant data security risks that extend beyond their own operations to impact clients. Hackers target law firms due to the valuable

[27] https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/.
[28] https://www.zorbsecurity.com/blog/legal-firm-data-theft-attacks-on-client-data/.

information they hold, such as trade secrets, intellectual property, personally identifiable information (PII), and confidential attorney-client-privileged data."[29]

81. "According to the American Bar Association's 2023 Legal Technology Survey, approximately 29% of law firms reported experiencing a data breach, up from 26% in 2022. Smaller firms are particularly at risk, with 35% of firms with 10-49 attorneys reporting breaches compared to 22% of firms with over 500 attorneys."[30]

82. Indeed, "[f]ive months into the year, 2024 is on pace to be the biggest year in the history of law firm data breach reports. At least 21 law firms filed data breach reports to state attorneys general offices this year. By comparison, 2023 saw 28 law firm breach reports, while 2022 had 33 breach reports and 2021 had 38."[31]

83. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its systems, yet it appears Defendant did not encrypt its systems, nor the information contained within them.

---

[29] https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2024/ensuring-security-protecting-your-law-firm-and-client-data/#:~:text=Law%20firms%20face%20significant%20data,attorney%2Dclient%2Dprivileged%20data.

[30] https://www.onelegal.com/blog/data-breaches-in-the-legal-industry/.

[31] https://www.law.com/americanlawyer/2024/05/23/law-firm-data-breach-reports-show-no-signs-of-slowing-in-2024/#:~:text=At%20least%2021%20law%20firms,report%20a%20breach%20this%20year.

84. It is recommended law firms institute the following best practices to protect client data:

a. Create and implement a data security policy;

b. Continuously train staff on mitigating data risk;

c. Use strong passwords;

d. Encrypt data;

e. Secure communications;

f. Consider access controls;

g. Conduct regular reviews;

h. Vet vendors carefully; and

i. Set up two-factor authentication.[32]

85. WLG failed to implement or follow one or more of the above best practices, resulting in the Data Breach.

86. As a law firm within the legal services industry, Defendant should have known about its data security weaknesses and sought better protection for the Private Information maintained on its systems.

[32] https://www.clio.com/blog/data-security-law-firms/.

F. Cybercriminals Will Use Plaintiff's and Class Members' Private Information to Defraud Them.

87. Plaintiff and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach will be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

88. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[33] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[34] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

---

[33]"Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[34]*See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

89. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[35]

90. For example, it is believed that certain Private Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[36]

91. This was a financially motivated Data Breach, as made apparent from the data encryption tactic the cybercriminals used. "Once the attacker gains access to the target system, they proceed to encrypt valuable information, such as personal details, credit card information, or account credentials, which can fetch them monetary rewards…After encrypting the data, the threat actors demand a ransom to release the private key required for decryption. Ransoms are typically demanded in cryptocurrencies like Bitcoin or Ethereum, offering a degree of anonymity to the attackers. It is important to note that paying the ransom does not guarantee the release of the private key, and there is no guarantee that the cycle of attacks and ransom demands will cease."[37]

---

[35] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[36] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[37] https://www.encryptionconsulting.com/understanding-how-cybercriminals-hold-

92. To date, there is no indication that Defendant has made any attempt to recover Plaintiff's and Class Members' Private Information.

93. The only reason cybercriminals go through the trouble of hacking law firms like WLG is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

94. The Private Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

95. "Stolen data is one of the fastest-selling commodities available on the dark web. There is an array of affordable hacking and exploitation tools at the disposal of petty fraudsters and sophisticated hackers alike. It has become all too easy to gain large profits from selling breached data on the dark web."[38]

96. "For people with high credit scores, a Social Security number, birth date, and full name can sell for $60 to $80 on the digital black market."[39]

---

your-data-hostage/#:~:text=Modern%20ransomware%20employs%20hybrid%20encryption,private%20key%20required%20for%20decryption.

[38] https://www.totalprocessing.com/how-much-is-your-data-worth-on-the-dark-web/

[39] https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web

97. Cybercriminals often bundle and sell information in "fullz" packages containing names, Social Security numbers, birth dates, account numbers and other data that make them desirable since they can often do a lot of immediate damage.[40]

98. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, ***they will use it***.[41]

99. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[42]

100. When cybercriminals manage to steal Social Security numbers and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

---

[40] https://www.breachsecurenow.com/what-is-your-personal-information-worth-on-the-dark-web/.

[41] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[42] *See Cases Currently Under Investigation,* U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

101. "ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC."[43]

102. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[44]

103. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

104. Victims of the Data Breach, like Plaintiff and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[45]

105. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions,

[43] https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[44] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[45] *Id.*

healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

106. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Private Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Private Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant' untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

107. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class Members' Private Information.

108. Plaintiff and Class Members are desperately trying to mitigate the damage that Defendant has caused them but, given the Private Information Defendant made accessible to cybercriminals, they are certain to incur additional

damages. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[46]

109. None of this should have happened. The Data Breach was entirely preventable.

G. WLG Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Private Information.

110. Data breaches are preventable.[47] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[48] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[49]

---

[46] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[47] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[48] *Id.* at 17.
[49] *Id.* at 28.

111. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[50]

112. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

113. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of

[50] *Id.*

data being transmitted from the system; and have a response plan ready in the event of a breach.[51]

114. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

115. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

116. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July

[51] *Protecting Private Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

117. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

118. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

119. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

120. Defendant required Plaintiff and Class Members to surrender their Private Information—including but not limited to their names and Social Security numbers—and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such Private Information.

121. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

122. Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

123. Defendant maintained Plaintiff's and the Class's Private Information in a reckless manner. In particular, their Private Information was maintained and/or exchanged, unencrypted, in Defendant's systems which were maintained in a condition vulnerable to cyberattacks.

124. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach.

125. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps

to secure Plaintiff's and Class Members' Private Information from those risks left that information in a dangerous condition.

126. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its systems and software were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

127. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

128. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Nationwide Class, defined as follows:

Nationwide Class

All persons residing in the United States who were victims of the Data Breach, including all of those who were sent a Notice of Data Breach letter from Defendant (the "Class").

129. Plaintiff reserves the right to amend the above definition(s) or to propose alternative or add subclasses in subsequent pleadings and motions for class certification.

130. The proposed Nationwide Class and Subclass (collectively referred to herein as the "Class" unless otherwise specified) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

131. **Numerosity:** The proposed Class is believed to be so numerous that the joinder of all members is impracticable. Joinder of all members would be impractical because it is comprised of hundreds of individuals.

132. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class Member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Defendant.

133. **Adequacy:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class she seeks to represent;

Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

134. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

135. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant's computer systems, software, and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act and/or state laws and/or Defendant' other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Private Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continue to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant' negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant' actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

136. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

137. Defendant solicited, gathered, and stored the Private Information of Plaintiff and the Class as part of the operation of its business.

138. Upon accepting and storing the Private Information of Plaintiff and Class Members, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

139. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

140. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in Defendant' possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

141. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

142. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

143. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a) To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to

ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b) To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c) To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

144. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

145. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to train its employees as to how to detect and avoid phishing emails;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

e. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

f. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Private Information;

g. Failing to mitigate the harm caused to Plaintiff and the Class Members;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

i. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

146. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

147. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

148. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

149. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

150. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, paying for spyware removal, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, and credit reports.

151. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

152. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

153. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

154. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

155. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class.

156. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

157. Defendant gathered and stored the Private Information of Plaintiff and the Class as part of its business which affect commerce.

158. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

159. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

160. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

161. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

162. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

163. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

164. Additionally, Defendant had a duty to promptly notify Plaintiff and the Class of the Data Breach. Defendant did not begin sending Notice of Data Breach Letters to Plaintiff and Class Members until on or around August 2024, despite knowing of the Breach as early as March 2024.

165. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

166. Defendant's violations of the FTC Act constitutes negligence *per se*.

167. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

168. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

169. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

COUNT THREE
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Class)

170. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

171. Plaintiff and Class Members reasonably expected that the sensitive Private Information entrusted to Defendant would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

172. Defendant unlawfully invaded the privacy rights of Plaintiff and Class Members by:

a) Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b) Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c) Enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

173. A reasonable person would find it highly offensive that Defendant, having collected Plaintiff's and Class Members' sensitive Private Information, failed to protect such Private Information from unauthorized disclosure to third parties.

174. In failing to adequately protect Plaintiff's and Class Members' sensitive Private Information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and Class Members' position.

175. Defendant violated Plaintiff's and Class Members' right to privacy under the common law.

176. Defendant's unlawful invasions of privacy damaged Plaintiff and the Class. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiff and Class Members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiff and the Class seek actual and nominal damages for these invasions of privacy.

COUNT FOUR
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

177. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

178. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

179. Through the use of Defendant's legal services, Defendant received monetary benefits from Plaintiff and the Class.

180. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it.

181. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with Plaintiff and the Class Members, knowingly and deliberately enriched itself by saving the costs it

reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiff's and Class Members' Private Information.

182. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among law firms entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members.

183. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of Private Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

184. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable,

unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

185. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

COUNT FIVE
BREACH OF IMPLIED CONTRACT
(On Behalf Plaintiff and the Nationwide Class)

186. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

187. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information, including their Social Security numbers and other sensitive personal information, as part of Defendant's regular business practices.

188. Plaintiff and Class Members were required to provide their Private Information to Defendant in order to receive legal services. Plaintiff and Class Members paid money to Defendant in exchange for legal services.

189. Defendant solicited and accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing legal services.

190. In delivering, directly or indirectly, their Private Information to Defendant and paying for legal services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their Private Information.

191. Plaintiff and Class Members reasonably expected that the Private Information they entrusted to WLG, in order to receive legal services would remain confidential and would not be shared or disclosed to criminal third parties.

192. Plaintiff and Defendant had a mutual understanding that WLG would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiff's and Class Members' sensitive Private Information. Plaintiff and Defendant also shared an expectation and understanding that WLG would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

193. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and Class Members' Private Information, Defendant had a duty to safeguard the Private Information in its possession through the use of reasonable data security practices.

194. When Plaintiff and Class Members paid money and provided their Private Information to WLG in exchange for goods or services, they entered into implied contracts with Defendant.

195. Defendant entered into implied contracts with Plaintiff and the Class under which Defendant agreed to comply with its statutory and common law duties to safeguard and protect Plaintiff's and Class Members' Private Information and to timely notify Plaintiff and Class Members of a data breach.

196. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act and other state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

197. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized medical purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi) requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

198. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such implied contracts.

199. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiff and Class Members.

200. Had Defendant disclosed to Plaintiff and Class Members that it did not have adequate data security practices to secure their Private Information, Plaintiff and Class Members would not have provided their Private Information to Defendant.

201. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

202. Defendant breached the implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

203. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it solicited and collected Plaintiff's and Class Members' Private Information.

204. Plaintiff and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

COUNT SIX
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

205. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

206. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, (i) to act primarily for Plaintiff and Class Members, (ii) for the safeguarding of their Private Information; (iii) to timely notify Plaintiff and Class Members of a data breach's occurrence and disclosure; and (iv) to maintain complete and accurate records of what information (and where) Defendant did and does store.

207. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its clients to keep their Private Information secure.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiff and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

209. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

210. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

211. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

212. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

213. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk

to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

COUNT SEVEN
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff incorporates by reference the allegations in paragraphs 1–135 as though fully set forth herein.

215. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

216. As previously alleged, Defendant was required to provide adequate security for the PII collected from Plaintiff and the Class.

217. Defendant owed and still owes a duty of care to Plaintiff and Class Members that require them to adequately secure Plaintiff's and Class Members' PII.

218. Upon reason and belief, Defendant still possesses the PII of Plaintiff and the Class Members.

219. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

220. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

221. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

222. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

223. There is no reason to believe that Defendant's data security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

224. Plaintiff and the Class, therefore, seek a declaration (i) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (ii) that to comply with its contractual

obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a) Ordering Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b) Ordering Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c) Ordering Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d) Ordering Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e) Ordering Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f) Ordering Defendant conduct regular database scanning and security checks; and

g) Ordering Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Defendant' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant' systems is compromised, hackers cannot gain access to other portions of Defendant' systems;

v. Ordering that Defendant cease transmitting Private Information via unencrypted email;

vi. Ordering that Defendant cease storing Private Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: August 22, 2024

Respectfully submitted,

/s/ Vicki J. Maniatis
Vicki J. Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (865) 412-2700
vmaniatis@milberg.com

David K. Lietz (*Pro Hac Vice forthcoming*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

William B. Federman
(*pro hac vice application forthcoming*)
Kennedy M. Brian
(*pro hac vice application forthcoming*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com